

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46

RICHFIELD PUBLIC SCHOOLS
ELECTRONIC USE AND COMMUNICATIONS

I. PURPOSE

The purpose of this policy is to set forth guidelines for access to and appropriate use of the Richfield Public School District's digital technologies and wireless and wired computer network systems. This includes, but is not limited to, acceptable and safe use of District-provided devices for student academic use.

II. GENERAL STATEMENT OF POLICY

In making decisions regarding employee and student access to the District's digital technologies, wireless and wired computer network systems, and software applications, including electronic communications, the District considers its own stated educational mission, goals, and objectives -- digital literacy, fluency, and citizenship, along with electronic information research skills are fundamental to the preparation of citizens and future employees. Access to the District's computer systems and to the internet enables students and employees to explore thousands of resources while communicating and collaborating with people around the world. The school district expects that all users will blend thoughtful use of the District's computer system and the internet throughout curriculum and instruction and will provide guidance to students in their use.

III. DEFINITIONS

- A. Communications equipment and networks: includes, but is not limited to, telephones (VoIP), voicemail, fax machines, desktop and laptop computers, Chromebooks, tablets, computer networks, email, and the internet.
- B. Electronic communications: The sharing of information and ideas through the use of electronic communications devices and internet applications. Electronic communications may have a permanency like that of paper communication and may be traceable to the sender. Applicable modes of communication include, but are not limited to, telephone/cell phone, voicemail, fax transmissions, computers, software, phone and computer applications, operating systems, computer networks, email, storage media, file transfer protocol (FTP), portable electronic devices, social media, and the internet.

- 1 C. Intellectual property: An individual's own thoughts and ideas
2 expressed through a product such as a drawing or written document
3 which may be viewed in the form of a tangible, "hard copy" such as
4 paper or stored electronically and viewed on a monitor or screen.
5 Student homework and teacher-created curricular items are specific
6 examples.
7
- 8 D. Internet: A world-wide network of computers. Internet access is
9 viewed both as an extension of the District's email and as an extension
10 of the schools' digital resources. This includes email, the World Wide
11 Web, social media, streaming media, and other similar electronic
12 content.
13
- 14 E. Copyright: The exclusive right granted by the federal government to
15 reproduce, publish, and sell the matter and form of a literary, musical,
16 or artistic work. Permission must be received from copyright holders
17 before copyrighted works can be used by others.
18
- 19 F. Fair use: A copyright law doctrine which permits educational
20 organizations and staff rights to legal, non-licensed citation or
21 incorporation of copyrighted materials within the confines of the
22 educational environment for criticism, comment, and instructional
23 purposes.
24
- 25 G. Eligible students: All rights and protections given parents/guardians
26 under this policy transfer to the student when the student reaches
27 eighteen (18) years of age or enrolls in an institution of post-secondary
28 education. The student then becomes an "eligible student." However,
29 the parents/guardians of an eligible student who is also a "dependent
30 student" are entitled to gain access to the educational records of such
31 student without first obtaining the consent of the student.
32
- 33 H. Access: Refers to a staff or student's rights to hardware and software
34 provided by Richfield Public Schools. Access can be altered or even
35 denied if a user violates this or other Board Policies.
36
- 37 I. Bullying: Refer to Board Policy 113 (Bullying Prohibition Policy)
38

39 **IV. LIMITED EDUCATIONAL PURPOSE**
40

41 The District is providing students and employees with access to the District's
42 digital network system, hardware, and software, which includes internet
43 access. The purpose of the District's digital network system is more specific
44 than providing students and employees with general access to the internet.
45 District communication systems and resources have limited educational
46 purposes, which include the use of the resources and system for classroom
47 activities, educational research, and professional or career development.

1 Users are expected to use access through the District's digital network
2 resources and system to further educational and personal goals consistent
3 with the mission of the school district and school policies. Uses which might
4 be acceptable to a user's private personal account or equipment on another
5 system may not be acceptable on this limited-purpose system.
6

7 **V. PROHIBITED USES**

8
9 A. While not an exhaustive list, the following uses of the District's system,
10 hardware, software, and internet resources or accounts are considered
11 unacceptable:
12

13 1. Users will not use the District's system to access, review,
14 upload, download, store, print, post, receive, transmit, or
15 distribute:
16

17 a. pornographic, obscene, or sexually explicit material or
18 other visual depictions that are harmful to minors;
19

20 b. obscene, abusive, profane, lewd, vulgar, rude,
21 inflammatory, threatening, disrespectful, or sexually
22 explicit language;
23

24 c. materials that use language or images that are
25 inappropriate in the education setting or disruptive to the
26 educational process;
27

28 d. information or materials that could cause damage or
29 danger of disruption to the educational process;
30

31 e. materials that use language or images that advocate
32 violence or discrimination toward other people (hate
33 literature) or that may constitute harassment or
34 discrimination.
35

36 2. Users will not use the District's system to knowingly or
37 recklessly post, transmit, or distribute false or defamatory
38 information about a person or organization, or to harass another
39 person, or to engage in personal attacks, including prejudicial or
40 discriminatory attacks.
41

42 3. Users will not use the District's system to engage in any illegal
43 act or violate any local, state, or federal statute or law.
44

45 4. Users will not use the District's system to vandalize, damage, or
46 disable the property of another person or organization, will not
47 make deliberate attempts to degrade or disrupt equipment,

- 1 software, or system performance by spreading computer
2 viruses or by any other means, will not tamper with, modify, or
3 change the District's system software, hardware, or wiring or
4 take any action to violate the District's security system, and will
5 not use the District's system in such a way as to disrupt the use
6 of the system by other users.
7
- 8 5. Users will not use the District's system to gain unauthorized
9 access to information resources or to access another person's
10 materials, information, or files without the implied or direct
11 permission of that person.
12
- 13 6. Users will not use the District's system to post private
14 information about another person, personal contact information
15 about themselves or other persons, or other personally
16 identifiable information, including, but not limited to, addresses,
17 telephone numbers, school addresses, work addresses,
18 identification numbers, account numbers, access codes or
19 passwords, unapproved labeled photographs, or other
20 information that would make the individual's identity easily
21 traceable, and will not repost a message that was sent to the
22 user privately without permission of the person who sent the
23 message.
24
- 25 a. This paragraph does not prohibit the posting of employee
26 contact information on the District's website or
27 communications between employees and other
28 individuals when such communications are made for
29 education-related purposes (i.e., communications with
30 parents or other staff members related to students).
31
- 32 b. Employees creating or posting school-related digital
33 presences may include personal contact information
34 about themselves on a webpage. However, employees
35 may not post personal contact information or other
36 personally identifiable information about students unless:
37
- 38 (1) such information is classified by the District's as
39 directory information and verification is made that
40 the District has not received notice from a
41 parent/guardian or eligible student that such
42 information is not to be designated as directory
43 information in accordance with Policy 581; or
44
- 45 (2) Such information is not classified by the District as
46 directory information but written consent for
47 release of the information to be posted has been

1 obtained from a parent/guardian or eligible student
2 in accordance with Policy 581.

3
4 In addition, prior to posting any personal contact
5 or personally identifiable information on a school-
6 related webpage, employees shall obtain written
7 approval of the content of the postings from the
8 building administrator or the District's Director of
9 Marketing & Communications.

10
11 c. These prohibitions specifically prohibit a user from
12 utilizing the school district system to post personal
13 information about a user or another individual on social
14 networks, including, but not limited to, "Facebook,
15 Twitter, Instagram, Snapchat, TikTok, etc."

16
17 7. Users will not attempt to gain unauthorized access to the
18 District's system or any other system through the District's
19 system, attempt to log in through another person's account, or
20 use computer accounts, access codes, or network identification
21 other than those assigned to the user. Messages and records
22 on the District's system may not be encrypted without the
23 permission of appropriate school authorities.

24
25 8. Users will not use the District's system to violate copyright laws
26 or usage licensing agreements, or otherwise to use another
27 person's property without the person's prior approval or proper
28 citation, including the downloading or exchanging of pirated
29 software or copying software to or from any school computer,
30 and will not plagiarize works they find on the internet.

31
32 9. Users will not use the District's system for conducting business,
33 for unauthorized commercial purposes, or for financial gain
34 unrelated to the mission of the District. Users will not use the
35 District's system to offer or provide goods or services or for
36 product advertisement, except for in the case of school-related
37 fundraisers.

38
39 10. Users will not use the District's system to engage in bullying or
40 cyberbullying in violation of the District's Bullying Prohibition
41 Policy 113. This prohibition includes using any technology or
42 other electronic communication off school premises to the
43 extent that student learning or the school environment is
44 substantially and materially disrupted.

45
46 B. The District has a special interest in regulating off-campus speech
47 that materially disrupts classwork or involves substantial disorder or

1 invasion of the rights of others. A student or employee engaging in
2 unacceptable use of the internet when off District premises also may
3 be in violation of this policy as well as other school district policies.
4 Examples of such violations may include, but are not limited to,
5 serious or severe bullying or harassment targeting particular
6 individuals; threats aimed at teachers or other students; failure to
7 follow rules concerning lessons, the writing of papers, the use of
8 computers, or participation in other online school activities; and
9 breaches of school security devices. If the District receives a report
10 of an unacceptable use originating from a non-school computer or
11 resource, the District may investigate such reports to the best of its
12 ability. Students or employees may be subject to disciplinary action
13 for such conduct, including, but not limited to, suspension or
14 cancellation of the use or access to the District computer system and
15 the internet and discipline under other appropriate District policies,
16 including suspension, expulsion, exclusion, or termination of
17 employment.

18
19 C. If a user inadvertently accesses unacceptable materials or an
20 unacceptable internet site, the user shall immediately disclose the
21 inadvertent access to an appropriate District official. In the case of a
22 District employee, the immediate disclosure shall be to the
23 employee's immediate supervisor and/or the building administrator.
24 This disclosure may serve as a defense against an allegation that the
25 user has intentionally violated this policy. In certain rare instances, a
26 user also may access otherwise unacceptable materials if necessary
27 to complete an assignment and if done with the prior approval of and
28 with appropriate guidance from the appropriate teacher or, in the
29 case of a District employee, the building administrator.

30
31 **VI. LIMITATIONS ON SCHOOL DISTRICT LIABILITY**

32
33 Use of the District's system is at the user's own risk. The system is provided
34 on an "as is, as available" basis. The District will not be responsible for any
35 damage users may suffer, including, but not limited to, loss, damage, or
36 unavailability of data stored on District hard drives, cloud services, or servers
37 (physical or virtual), or for delays or changes in or interruptions of service or
38 misdeliveries or nondeliveries of information or materials, regardless of the
39 cause. The District is not responsible for the accuracy or quality of any advice
40 or information obtained through or stored on the school district system. The
41 District will not be responsible for financial obligations arising through
42 unauthorized use of the school district system or the internet.

43
44 **VII. INTERNET SAFETY**

45
46 The District will employ technical systems designed to restrict and monitor
47 access to materials harmful to minors, including but not limited to internet

1 filtering systems. Access to systems such as email and social media will be
2 limited to curriculum-related work only.

3
4 A. With respect to any of its computers with internet access, the District
5 will monitor the online activities of both minors and adults and employ
6 technology protection measures during any use of such computers by
7 minors and adults. The technology protection measures utilized will
8 block or filter internet access to any visual depictions that are:

- 9
10 1. Obscene;
11
12 2. Child pornography;
13
14 3. Harmful to minors; or
15
16 4. Detrimental to, or obstructive of a student's ability to learn in a
17 safe, productive environment.

18
19 B. The term "harmful to minors" means any picture, image, graphic image
20 file, or other visual depiction that:

- 21
22 1. Taken as a whole and with respect to minors, appeals to a
23 prurient interest in nudity, sex, or excretion; or
24
25 2. Depicts, describes, or represents, in a patently offensive way
26 with respect to what is suitable for minors, an actual or
27 simulated sexual act or sexual contact, actual or simulated
28 normal or perverted sexual acts, or a lewd exhibition of the
29 genitals; and
30
31 3. Taken as a whole, lacks serious literary, artistic, political, or
32 scientific value as to minors.

33
34 C. Software filtering technology shall be narrowly tailored and shall not
35 discriminate based on viewpoint.

36
37 D. An administrator, supervisor, or other person authorized by the
38 superintendent may disable the technology protection measure, during
39 use by an adult, to enable access for bona fide research or other
40 lawful purposes.

41
42 E. The District will educate students about appropriate online behavior,
43 including interacting with other individuals on social networking
44 websites and will actively train students on digital fluency, literacy, and
45 cyberbullying awareness and response.

46
47 **VIII. PRIVACY EXPECTATIONS**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47

- A. The District maintains control of the materials on its systems contained in files on the system. Users should not expect privacy in the contents of personal files on the District's systems. Files stored on District computers and servers should not be considered the private property of individuals and may be viewed by supervisory school employees.
- B. Routine maintenance and monitoring of District systems may lead to a discovery that a user has violated this policy, another District policy, or the law.
- C. An individual investigation or search will be conducted if school authorities have a reasonable suspicion that the search will uncover a violation of law or District policy.
- D. Parents/guardians may have the right at any time to investigate or review the contents of their child's files and email files by way of written request in accordance with Policy: 581: Protection and Privacy of Pupil Records.
- E. District employees should be aware that the District retains the right at any time to investigate or review the contents of their files and email files. In addition, District employees should be aware that data and other materials in files maintained on the school district system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).
- F. The District will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with District policies conducted through the District's systems.

IX. USER NOTIFICATION

- A. All users shall be notified of the District's policies relating to the use of the District's digital network system and internet use.
- B. This notification shall include the following:
 - 1. Notification that use of the District's digital network system and internet use is subject to compliance with District policies.
 - 2. Disclaimers limiting the District's liability relative to:
 - a. Information stored on District hard drives, cloud-based storage, or servers.

- 1 b. Information retrieved through District computers,
2 networks, or online resources.
- 3
- 4 c. Personal property used to access District computers,
5 networks, or online resources.
- 6
- 7 d. Unauthorized financial obligations resulting from use of
8 District resources/accounts to access the internet.
- 9
- 10 3. A description of the privacy rights and limitations of school
11 sponsored/managed internet accounts.
- 12
- 13 4. Notification that, even though the District may use technical
14 means to limit student and staff internet access, these limits do
15 not provide a foolproof means for enforcing the provisions of
16 this acceptable use policy.
- 17
- 18 5. Notification that goods and services can be purchased over the
19 internet that could potentially result in unwanted financial
20 obligations and that any financial obligation incurred by a
21 student through the internet is the sole responsibility of the
22 student and/or the student's parents/guardians.
- 23
- 24 6. Notification that the collection, creation, reception, maintenance,
25 and dissemination of data via the internet, including electronic
26 communications, is governed by Policy 412: Public and Private
27 Personnel Data, and Policy 581: Protection and Privacy of Pupil
28 Records.
- 29
- 30 7. Notification that, should the user violate the District's acceptable
31 use policy, the user's access privileges may be revoked, school
32 disciplinary action may be taken and/or appropriate legal action
33 may be taken.
- 34
- 35 8. Notification that all provisions of the acceptable use policy are
36 subordinate to local, state, and federal laws.
- 37

38 **X. PARENT/GUARDIAN RESPONSIBILITY; NOTIFICATION OF STUDENT**
39 **INTERNET USE**

- 40
- 41 A. Outside of school, parents/guardians bear responsibility for the same
42 guidance of internet use as they exercise with information sources
43 such as television, telephones, smartphones, tablets, personal
44 computers, radio, movies, streaming content, video games, and other
45 possibly offensive media. Parents/guardians are responsible for
46 monitoring their child's use of the District's system and of the internet if

- 1 the child is accessing the District's system from home or a remote
2 location.
3
4 B. Parents/guardians will be notified that their child will be using District
5 resources/accounts to access the internet. This notification should
6 include:
7
8 1. A copy of the user notification form provided to the student user.
9
10 2. A description of parent/guardian responsibilities.
11
12 3. A statement that the Internet Use Agreement must be digitally
13 or physically signed by the user and the parent or guardian prior
14 to use by the student.
15
16 4. A statement that the District's acceptable use policy is available
17 for parental review on the District website.
18

19 **XIII. IMPLEMENTATION; POLICY REVIEW**

- 20
21 A. The District administrators may develop appropriate user notification
22 forms, guidelines, and procedures necessary to implement this policy
23 for submission to the school board for approval. Upon approval by the
24 school board, such guidelines, forms, and procedures shall be an
25 addendum to this policy.
26
27 B. The administration shall revise the user notifications, including student
28 and parent/guardian notifications, if necessary, to reflect the adoption
29 of these guidelines and procedures.
30
31 C. The District's internet policies and procedures are available for review
32 by all parents, guardians, staff, and members of the community on the
33 District website.
34
35 D. Because of the rapid changes in the development of the internet, the
36 school board shall conduct an annual review of this policy.
37
38

39 ***Legal References:***

- 40
41 Minn. Stat. Ch. 13 (Minnesota Government Data Practices Act)
42 15 U.S.C. § 6501 *et seq.* (Children's Online Privacy Protection Act)
43 17 U.S.C. § 101 *et seq.* (Copyrights)
44 20 U.S.C. § 1232g (Family Educational Rights and Privacy Act)
45 47 U.S.C. § 254 (Children's Internet Protection Act of 2000 (CIPA))
46 47 C.F.R. § 54.520 (FCC rules implementing CIPA)
47 Minn. Stat. § 121A.031 (School Student Bullying Policy)

- 1 Minn. Stat. § 125B.15 (Internet Access for Students)
- 2 Minn. Stat. § 125B.26 (Telecommunications/Internet Access Equity Act)
- 3 *Mahanoy Area Sch. Dist. v. B.L.*, 594 U.S., 141 S. Ct. 2038 (2021)
- 4 *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969)
- 5 *United States v. Amer. Library Assoc.*, 539 U.S. 1942003)
- 6 *Sagehorn v. Indep. Sch. Dist. No. 728*, 122 F.Supp.2d 842 (D. Minn. 2015)
- 7 *R.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F.Supp.2d 1128 (D. Minn. 2012)
- 8 *Tatro v. Univ. of Minnesota*, 800 N.W.2d 811 (Minn. App. 2011), aff'd on other
- 9 grounds 816 N.W.2d 509 (Minn. 2012)
- 10 *S.J.W. v. Lee's Summit R-7 Sch. Dist.*, 696 F.3d 771 (8th Cir. 2012)
- 11 *Parents, Families and Friends of Lesbians and Gays, Inc. v. Camdenton R-III Sch.*
- 12 *Dist.*, 853 F.Supp.2d 888 (W.D. Mo. 2012)
- 13 *M.T. v. Cent. York Sch. Dist.*, 937 A.2d 538 (Pa. Commw. Ct. 2007)
- 14
- 15
- 16

Cross References:

- 17
- 18 Board Policy 103 (Harassment Prohibition)
- 19 Board Policy 109 (Distribution of Nonschool-sponsored Materials on School
- 20 Premises by Students and Employees)
- 21 Board Policy 113 (Bullying Prohibition)
- 22 Board Policy 412 (Public and Private Personal Data
- 23 Board Policy 452 (Evaluation and Development of Professional Staff)
- 24 Board Policy 451 (Student Discipline)
- 25 Board Policy 564 (School Records and Data Privacy)
- 26 Board Policy 581 (Protection and Privacy of Pupil Records)
- 27 Board Policy 601 (Curriculum and Instruction Goals)
- 28 Board Policy 607 (Online Learning Options)
- 29 Board Policy 608 (Students with Disabilities)
- 30 Board Policy 610 (Selection of Instructional Material)
- 31 Board Policy 611 (Provision for Alternative Instruction)
- 32 Board Policy 612 (Curriculum Management)
- 33 Board Policy 616 (School Sponsored Publications)
- 34 Board Policy 802 (Crisis Management)
- 35 Employee handbooks, collective bargaining agreements
- 36
- 37
- 38
- 39

40 RATIFIED BY THE BOARD OF EDUCATION: September 16, 1996

41

42 REVISED BY THE BOARD OF EDUCATION: August 23, 1999; October 15, 2001;

43 November 20, 2006; December 4, 2007; March 16, 2015; April 19, 2021; September

44 6, 2022

45

46 REVIEWED AND REAFFIRMED BY THE BOARD OF EDUCATION: February 5,

47 2001; August 16, 2021; September 5, 2023